



Local Agency Security Officer 2016

- KCJIS Overview
- LASO Responsibilities
- Policy Highlights
- Advanced Security Awareness Topics



BIFURCATE

intransitive verb : to divide into two branches or parts

Bifurcate derives from the Latin *bifurcus*, meaning "two-pronged,"



Kansas CCH

per K.S.A. 22-4701 et seq.

AFIS

K.I.B.R.S.

Nlets CTA

eDisposition

KsORT

K.I.S.

LPR downloads

KS DLs



KBI HELPDESK:

1-785-296-8245

helpdesk@kbi.state.ks.us



Training,
Audit,
Approvals



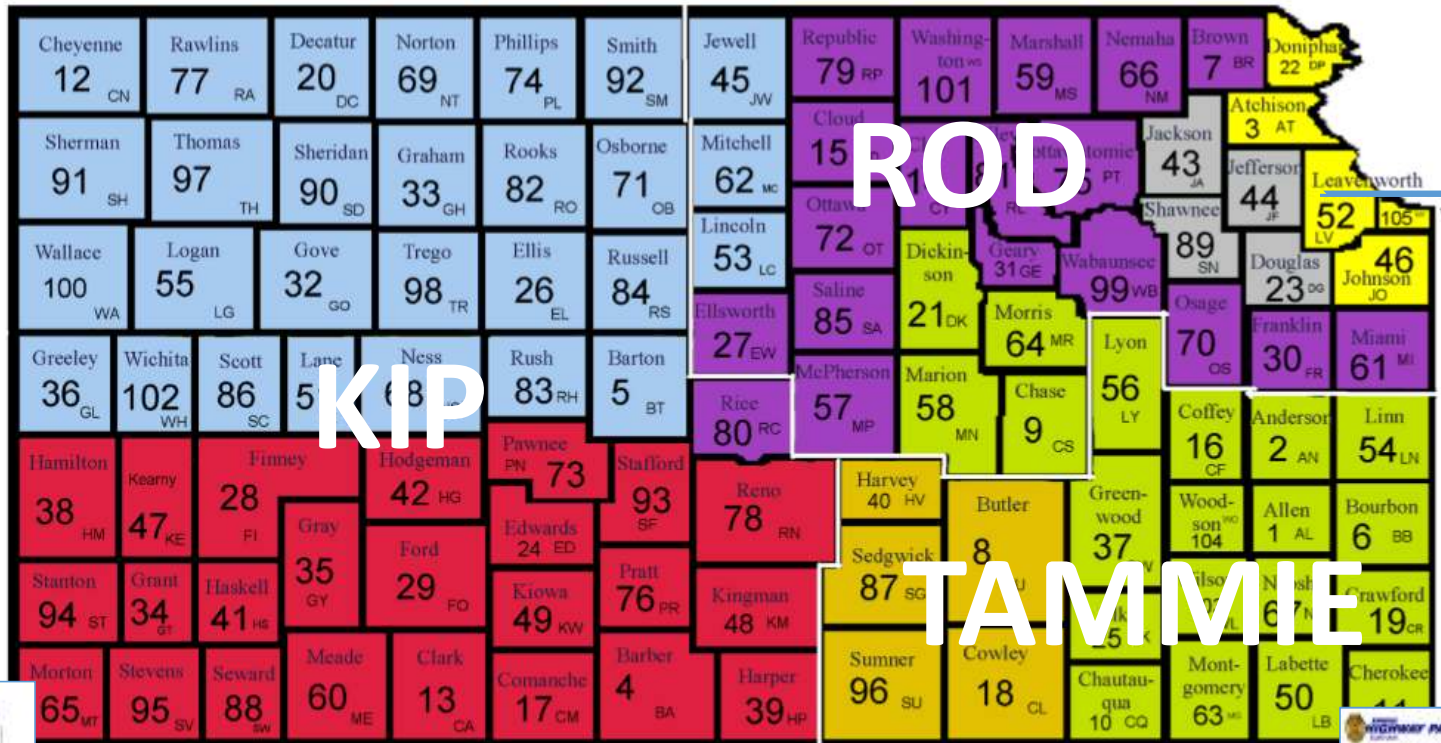
NCIC
III
N-DEx

<https://cjisaudit.khp.ks.gov> > CJIS Training > KCJIS TRAINER/AUDITOR MAP with Contact Information)



KANSAS
HIGHWAY PATROL
CJIS Unit

CONTACT INFORMATION



**Click on your county to find your
KHP CJIS Unit contact information**

[\(Or Click here for complete KCJIS Unit Directory\)](#)

Revised: February 18, 2016



What is needed to access ?



Checkpoint SecuRemote VPN

OR



firewall to firewall VPN



- KACIS
- KSMART
 - KIBRS
 - LAW
 - KS Warrants



KS Central Message Switch:

- NCIC
- III
- Nlets



- ❖ OpenFox
- ❖ Local CAD SW
- ❖ REJIS



What is needed to access ?



TLS (https)

- KANSAS ONLY CCH search
- KANSAS DL Photos
- eDisposition
- LPR Downloads



- LEEP
 - N-Dex
 - (2-factor authentication)
 - TLS 1.2
- FBI.gov (Public access)



The vendor for tokens has changed.

OPTIV Security

6130 Sprint Parkway, suite 400

Overland Park, KS 66211

Phone (sales) 888-732-9406

FAX 816-421-6677

tokens@optiv.com

TRAITS OF A



- NIMBLE

- QUICK

- FLEXIBLE



- COMFORTABLE WITH TECHNOLOGY

- PART ATTORNEY

- PART TEACHER



3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.
4. Ensure the approved and appropriate security measures are in place and working as expected.
1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
6. *The agency LASO is responsible for securing security awareness training and associated record keeping.*



3.2.9 Local Agency Security Officer (LASO)

Resources:

- ❖ KHP CJIS LAUNCH PAD <https://cjisaudit.khp.ks.gov/launchpad/index.pl>
- ❖ FBI CJIS Security Policy Resource Center <https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>
- ❖ KCJIS Secure Web Portal <https://kcjis.ks.gov>



3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.



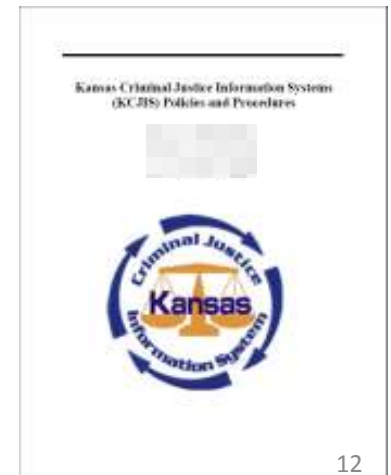
❖ KCJIS Policies and Procedures

- KCJIS has adopted the FBI CJIS Security Policy as the foundational document for KCJIS policies.
- Included as policy by reference are: Title 28 part 20, Code of Federal Regulations (CFR); The NCIC 2000 Operating Manual and associated Technical and Operational Updates (TOUs), The N-Dex Operations manual, and Kansas Statutes and Regulations.

❖ FBI CJIS Security Policy Version 5.5 6/1/2016

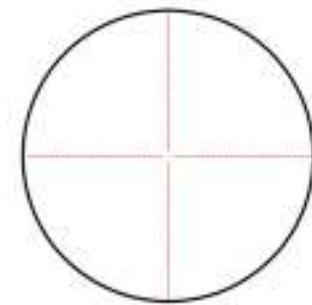
- FBI Requirements and Tiering Document lists the 568 “shall” statements

	Ver 5.3 Location and New Requirement	Ver 5.4 Location and New Requirement	Topic	Shall Statement	Requirement Priority Tier
	New 5.13.8	5.13.8	Wireless Hotspot Capability	When an agency allows mobile devices to function as a wireless access point, they shall be configured.	
547	New 5.13.8		-	1. In accordance with the requirements in section 5.13.1.1 All 802.11 Wireless Protocols	1
548	New 5.13.8		-	2. To only allow connections from agency authorized devices	1
549	New 5.13.9.1	5.13.9.1	Local Device Authentication	When mobile devices are authorized for use in accessing CJIS, local device authentication shall be used to unlock the device for use.	1
550	New 5.13.9.1		-	The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators	1
	New 5.13.10	5.13.10	Device Certificates	When certificates or cryptographic keys used to authenticate a mobile device are stored on the device, they shall be:	
551	New 5.13.10		-	1. Protected against being extracted from the device	1
552	New 5.13.10		-	2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts	1
553	New 5.13.10		-	3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use	1





SCOPE



WHAT	UNENCRYPTED CJI	4.1 ; 5.10.1.2
WHERE	TRUSTED NETWORK(S)	5.10 ; 5.7 ; 5.13
	PHYSICALLY SECURE LOCATION	5.9 ; 5.8
WHO	AUTHORIZED PERSONNEL	5.12 ; 5.2 ; 5.1 ; 5.5 ; 5.6

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS and KCJIS provided data necessary for law enforcement and civil agencies to perform their missions ...

KCJIS POLICIES and AUDIT are applicable if:

The source of the information is KCJIS.
“As if you are borrowing”.



Is your information mingled with KCJIS sourced information?



Protect information to highest level possible!
Or @least to highest applicable policy.

DIRECT



10-27



10-29



Ctrl + C

Ctrl + V



INDIRECT



RMS



Case #



<https://cjisaudit.khp.ks.gov>

The sequence of screenshots illustrates the navigation path within the CJIS Audit application:

- Top-Left Screenshot:** The 'Applications' menu on the left sidebar has 'CJIS Documents' circled in blue.
- Top-Right Screenshot:** The 'CJIS Documents' list on the right sidebar has 'KCJIS POLICIES and COMMITTEE (17)' circled in blue.
- Bottom-Left Screenshot:** The 'Kansas Criminal Justice Information Systems (KCJIS) Policies and Procedures' document is displayed, featuring the 'Criminal Justice Information Systems Kansas' logo.
- Bottom-Right Screenshot:** The 'Showing Documents in: KCJIS POLICIES and COMMITTEE' view shows 'KCJIS Policy and Procedures' circled in blue.

<https://kcjis.ks.gov>

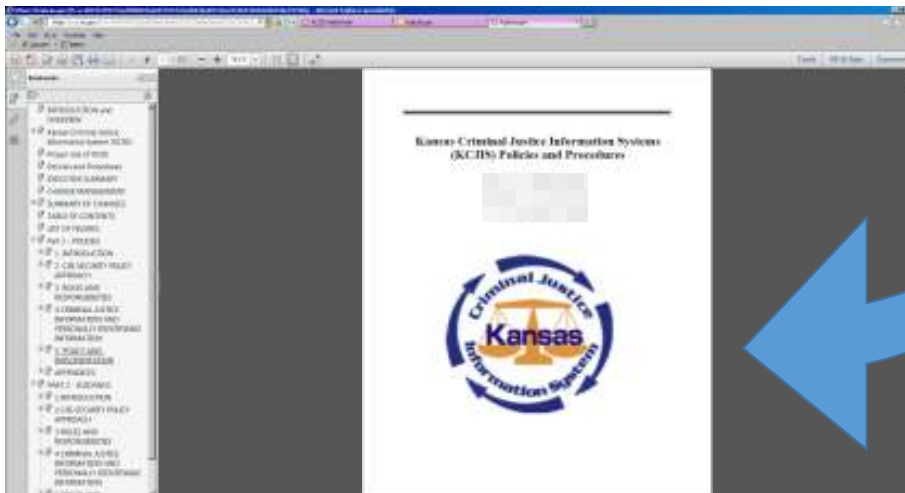
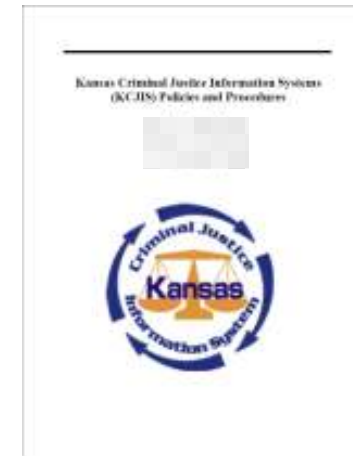


TABLE OF CONTENTS

INTRODUCTION and OVERVIEW	i
Kansas Criminal Justice Information System (KCJIS).....	i
Responsibilities	i
The KBI:	i
Criminal Justice Agencies:.....	ii
Proper Use of KCJIS.....	ii
Policies and Procedures	ii
EXECUTIVE SUMMARY	iii
CHANGE MANAGEMENT	iv
SUMMARY OF CHANGES	v
APB Approved Changes.....	v
Administrative Changes	vi
KCJIS Changes	viii
TABLE OF CONTENTS	ix
LIST OF FIGURES	xii
Part 1 - POLICIES.....	i
1 INTRODUCTION.....	1
1.1 Purpose.....	1
1.2 Scope	1
1.3 Relationship to Local Security Policy and Other Policies	1
1.4 Terminology Used in This Document	2
1.5 Distribution of Security Policy	2
2 CJIS SECURITY POLICY APPROACH	3
2.1 CJIS Security Policy Vision Statement	3
2.2 Architecture Independent	3
2.3 Risk Versus Realism	3
3 ROLES AND RESPONSIBILITIES	4
3.1 Shared Management Philosophy.....	4
3.2 Roles and Responsibilities for Agencies and Parties.....	4



1.3 Relationship to Local Security Policy and Other Policies


This Security Policy may be used as the sole security policy for the agency. The local agency may complement this Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, this Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from these Policy standards.

The KCJIS committee has chosen to adopt the FBI CJIS Security Policy as the baseline policy for KCJIS. When KCJIS requirements exceed those of FBI CJIS policy, the KCJIS language will be identified by a KCJIS icon in the left margin as illustrated in this paragraph.

Whenever the terms CJIS or NCIC are used in any part of this publication, it generally refers to both FBI CJIS and KCJIS provided information and systems used to access that information.

KCJIS Policies and Procedures -- 5.4
PART 1 POLICIES

1

KCJIS additions/enhancements in line on same page of FBI requirements. Notated by .

PART 2 - GUIDANCE

1 INTRODUCTION

- 1.1 Purpose
- 1.2 Scope
- 1.3 Relationship to Local Security Policy and Other Policies

2 CJIS SECURITY POLICY APPROACH

3 ROLES AND RESPONSIBILITIES

- 3.1 Shared Management Philosophy
- 3.2 Roles and Responsibilities for Agencies and Parties

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFO

- 4.1 Criminal Justice Information (CJI)
- 4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI),
Files Information, and NCIC Non-Restricted Files Information
- 4.3 Personally Identifiable Information (PII)

5 POLICY AND IMPLEMENTATION

1 INTRODUCTION

1.1 Purpose

1.2 Scope

1.3 Relationship to Local Security Policy and Other Policies

The local agency's Standard Operating Procedures (SOP) manual should include any specific instructions to facilitate the implementation of any local agency systems with specific focus on how to use the local systems in compliance with FBI and KCJIS policies. For example, if your agency utilizes a CAD/RMS system that accesses or stores CJI, your agency will need to have specific procedures for using that system.

Additionally, several phrases are used in the FBI policies to indicate the intent to require written procedures by local agencies. To assist in determining what local documentation is required the Kansas Highway Patrol CJIS unit searched the policies using keywords such as document, documentation, process, processes, and procedures. Furthermore, using the experience of FBI CJIS audits enforcement and interpretation of policy, the KHP audit unit has developed the following lists of required Standard Operating Procedures or policies that local agencies need to maintain:

SOP items verified during an NCIC/Data Quality compliance audit include the following:

- ☐ Procedures for dissemination of CJI and CHRI to authorized recipients.
- ☐ Procedure for verifying requestor of CJI is an authorized recipient prior to dissemination.
- ☐ Procedures for accommodating Individual Access & Review of one's own CHRI.
- ☐ Agency specific NCIC and KS Warrant File quality assurance procedures.
- ☐ Agency training policies and procedures regarding entry and query of records contained in the various state and federal systems accessed via KCJIS.
- ☐ Conducting Pre-employment record checks (see 5.12.1.1)
- ☐ Self-Reporting of new criminal violation (see 5.12.1)
- ☐ Reporting of Policy violations (see 5.3.6.1)
- ☐ Transfer or removal of personnel for violation of local or KCJIS policies.(See 5.12.3)
- ☐ Terminating access to KCJIS for resigned or suspended personnel. (See 5.12.2)
- ☐ Mobile Device Usage for accessing III.

The "Summary of Changes" page lists requirements that were added, deleted, or changed from the previous version and are now reflected in the current version. Within the document, the changes and additions are highlighted in yellow for ease of location.

- Tier 1 requirements must be met by a system before a CSO can allow connection to the state system.
- Tier 2 requirements must be met by the date indicated in the plan approved by the CSO.

Please refer questions or comments about this requirements document or the current version of the CJIS Security Policy to your respective Information Security Officer, CJIS Systems Officer, or Contact Officer.

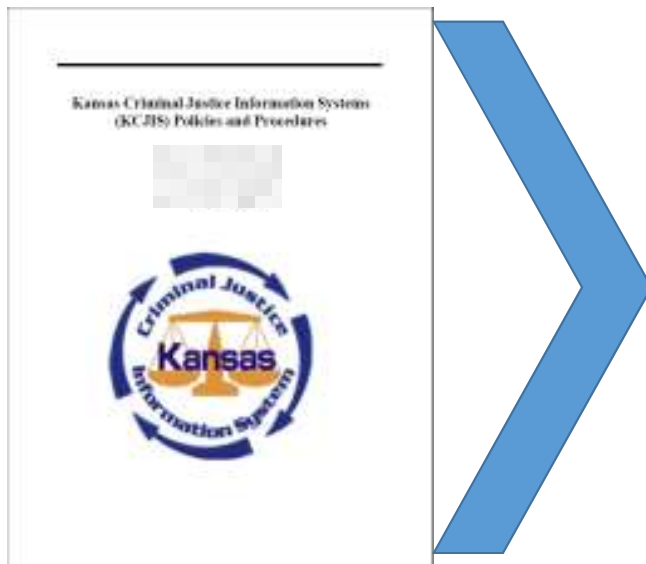
- Tier 1 requirements must be met by a system before a CSO can allow connection to the state system.
- Tier 2 requirements must be met by the date indicated in the plan approved by the CSO.

8	3.2.2(1)	3.2.2(1)	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJIS.	1
9			"	2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJJ, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.	1
10			"	a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.	1
11			"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.	1
12	3.2.2(2)	3.2.2(2)	"	c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.	1
13			"	d. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.	1
14			"	e. Ensure each agency having access to CJIS has someone designated as the Local Agency Security Officer (LASO).	1
15			"	f. Approve access to FBI CJIS systems.	1
16			"	g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.	1
17			"	h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.	1
	3.2.2(3)		"	3. Outsourcing of Criminal Justice Functions	
18	3.2.2(3)	3.2.3(3)	"	a. Responsibility for the management of the approved security requirements shall remain with the CIA.	1

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

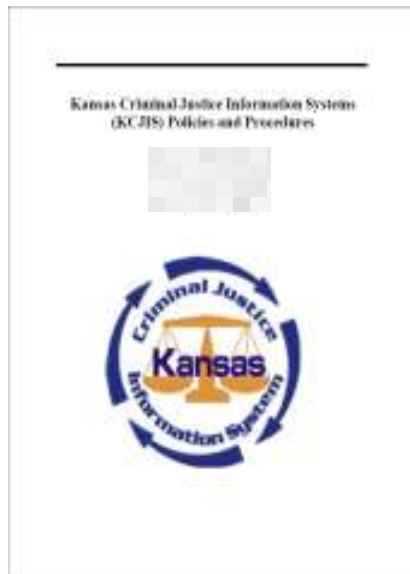


	Ver 5.4 Location & New Requirement	Topic	Shall Statement	Requirement Priority Tier
37	3.2.9	"	2. Identify and document how the equipment is connected to the state system.	1
38		"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.	1
39		"	4. Ensure the approved and appropriate security measures are in place and working as expected.	1
40		"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.	1
		"	6. The agency LASO is responsible for securing security awareness training and associated record keeping.	
		"	Agencies shall make notification to the Kansas Highway Patrol CJIS Unit within 3 business days of a LASO change within their agency.	
		FBI CJIS Division Information Security Officer (FBI)	The FBI CJIS ISO shall:	

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.



	Ver 5.4 Location & New Requirement	Topic	Shall Statement	Requirement Priority Tier
385	5.10.1	Information Flow Enforcement	The network infrastructure shall control the flow of information between interconnected systems.	1
386	5.10.1.1	Boundary Protection	The agency shall :	
387		"	1. Control access to networks processing CJI.	1
		"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.	1
		"	3. KCJIS policy requires that any connections to the Internet, other external networks, or non-criminal justice information systems occur through locally managed firewalls. See Section 5.13.4.4 for guidance on personal firewalls. Also refer to National Institute of Standards and Technology (NIST) Special Publication 800-41 Guidelines on Firewalls and Firewall Policy, available at http://www.nist.gov/customrf/get_pdf.cfm?pub_id=901083 .	1
389		"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.	1
390		"	5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").	1
391		"	6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in section 5.10.3.2 to achieve separation.	1
392		Encryption	1. Encryption shall be a minimum of 128 bit.	1

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

5.11 Policy Area 11: Formal Audits

5.11.2.2 Triennial Security Audits by the Kansas Highway Patrol CJIS Unit

❖ Based on KCJIS Policies and Procedures

- FBI CSP
- KCJIS additions
- Requirements and Tiering Document lists the “shall” statements.

❖ Your Information Technology Security Auditor will contact you “when it’s time”.

❖ Complete the questionnaire your auditor will provide.

- On site will go quicker

❖ On site visit to confirm physical security and hardware.

❖ Excellent time for 1 to 1 training and questions answered.



	Ver 5.4 Location & New Requirement	Topic	Shall Statement	Requirement Priority Tier
385	5.10.1	Information Flow Enforcement	The network infrastructure shall control the flow of information between interconnected systems.	1
		Boundary Protection	The agency shall :	
386		"	1. Control access to networks processing CJI.	1
387		"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.	1
		"	3. KCJIS policy requires that any connections to the Internet, other external networks, or non-criminal justice information systems occur through locally managed firewalls. See Section 5.13.4.4 for guidance on personal firewalls. Also refer to National Institute of Standards and Technology (NIST) Special Publication 800-41 Guidelines on Firewalls and Firewall Policy, available at http://www.nist.gov/customers/get_pdf.cfm?pub_id=901063 .	1
389	5.10.1.1	"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.	1
390		"	5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device shall "fail closed" vs. "fail open").	1
391		"	6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in section 5.10.3.2 to achieve separation.	1
392		Encryption	1. Encryption shall be a minimum of 128 bit.	1

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

5.3.1 Reporting Information Security Events

Providing DETAILS will help us help you get back up and running ASAP.

- If your anti-virus reported detected malware- what did it call it?
 - Different malware can be handled accordingly IF we know what it is.
- Who's device?
- How did they get infected?
- How are you going to keep it from happening again?

26

5.3 Policy Area 3: Incident Response

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, **and recovery**.

Damage mitigation =



- SCHEDULED (automated recommended)
- Limit access to administrators

Workstation to server or external media?

- Network is easy to restore quickly if file inadvertently deleted
 - Who keeps track of individual media?
-
- BACKUP to external media or site
 - All data needed for operations
 - Separate path and access controls than user
 - ENCRYPTED with agency holding keys
 - 4.2.4; 5.8.1; 5.8.2; Storage & transport of CJI
 - 5.1 Agreements
 - 5.12 Personnel screening
 - 5.2 Security awareness training
 - 5.10.1.2 Encryption
 - 5.10.1.5 Cloud Computing (stay tuned for future)



3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

4. Ensure the approved and appropriate security measures are in place and working as expected.

What about other entities allowed to access CJI or your systems?



5.1 Policy Area 1: Information Exchange Agreements

WHO are you allowing to access information?

HOW will it be adjudicated/enforced?

- Governmental Agency – 5.1.1.4 Agreements
 - Governmental - Paper, cease access w/ notice.
- Private Contractor – 5.1.1.5 Contract
 - Obligated to term for Payment & Civil Court for disputes.
 - See policy **3.2.7 Agency Coordinator (AC)**

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

4. Ensure the approved and appropriate security measures are in place and working as expected.



5.4 Policy Area 4: Auditing and Accountability

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system.

The **agency's information system** shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

- 5.5 Policy Area 5: Access Control
- 5.6 Policy Area 6: Identification and Authentication

- ☐ **KACIS**

COMING - SPRING 2017

Identity and Access Management

- ☐ **OpenFox Configurator**



5.5 Policy Area 5: Access Control

Who can get to what? (Authorized Access ONLY)

The KBI:

- Ensures maximum availability of KCJIS and accuracy of KCJIS information.
- **Administers** and maintains the core **KCJIS** servers, *including the network, related security, technical help desk, hardware, software and interfaces.*
- Hosts the state central repository as defined in K.S.A. 22-4701 et. seq.



is covered in TAC training.

HEADS UP!

WAIT FOR IT...

IDENTIFICATION and ACCESS Management

5.12.2 Personnel Termination

The agency, upon termination of individual employment, shall immediately terminate access to CJI.

5.5.1 Account Management

... The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.



5.6 Policy Area 6: Identification and Authentication

5.6.2.1 Standard Authenticators

5.6.2.1.1 Password

In 2014 FBI audit, we learned:

- **Password policy needs to be applied at some point prior to accessing CJI systems.**
 - **Device authentication (Windows)**
 - **CJI application access (CAD/RMS)**
- **Make sure ALL required attributes/rules are being applied**
 - **Robust - 8 or more characters, not dictionary word or name, not same as userid,**
 - **Expiration – expires within 90 days**
 - **History – can't use same password for 10 changes**

5.6 Policy Area 6: Identification and Authentication

5.6.2.1 Standard Authenticators

5.6.2.1.2 Personal Identification Number (PIN)

When agencies utilize a PIN in conjunction with a certificate or **a token** (e.g. key fob with rolling numbers) **for the purpose of advanced authentication**, agencies shall follow the PIN attributes described below

1. **Be a minimum of six (6) digits**
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. **Expire within a maximum of 365 calendar days.**
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.



(with version 5. 3)

5.6 Policy Area 6: Identification and Authentication

LOCAL CAD/RMS?

5.6.2.2.1 Advanced Authentication Policy and Rationale

...

AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), **or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access)**



(version 5. 4)

NO A.A. required by FBI or KCJIS { Lockable patrol car = “physically secure location”
Electronic RMS is a local agency database (not KCJIS) = “indirect access” to CJI

If your agency, county or city decide A.A. is appropriate:

Use 5.6.2.2 and Figure 8 = Advanced Authentication Use Cases for guidance.

And remember KCJIS ACCESS STILL REQUIRES RSA SecureID Token Advanced Authentication.



5.6 Policy Area 6: Identification and Authentication

LOCAL CAD/RMS?

5.6.2.2.1 Advanced Authentication Policy and Rationale

2 Case studies of a patrol officer with an MDT in their patrol car.

1. Officer runs own 27, 28, etc.
 - a. Unique username + password for MDT/agency resources
 - b. KCJIS User ID + PIN + TOKEN still required to access anything at or through KCJIS.
2. Officer only receives dispatches and enters information such as arrival time, narratives, and information obtained on scene.
 - a. Unique username + password for MDT/agency resources



3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

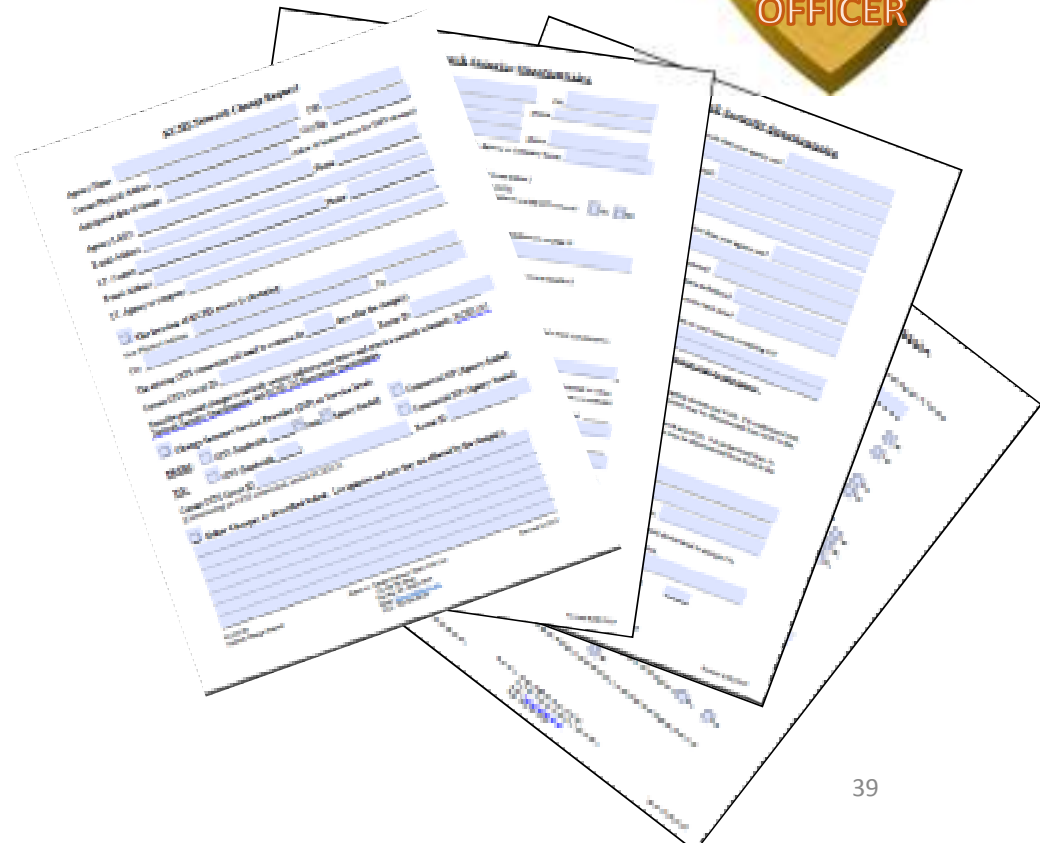
- 2. Identify and document how the equipment is connected to the state system.**



5.7 Policy Area 7: Configuration Management

5.7.1.2 Network Diagram

- ☐ **CURRENT**
- ☐ **Shows interconnectivity and separation of CJA from NCJA**
- ☐ **“For Official Use Only ” to mitigate KORA, etc.**
- ☐ **KCJIS 129 Network change request PACKET**



3.2.9 Local Agency Security Officer (LASO)

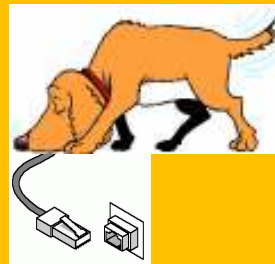
Each LASO shall:

3. Ensure that personnel security screening procedures are being followed as stated in this Policy.



5.12 Policy Area 12: Personnel Security

- ☐ Within 30 days for government employee assignment with DIRECT ACCESS to CJI systems.
- ☐ BEFORE contractor employee is granted ANY ACCESS to unencrypted (plaintext) CJI.
- ☐ Anyone with “roamin’ around” access to areas where CJI is processed or stored.
- ☐ Anyone with unmonitored access to networks used to transmit unencrypted CJI.



5.12 Policy Area 12: Personnel Security



Why different?

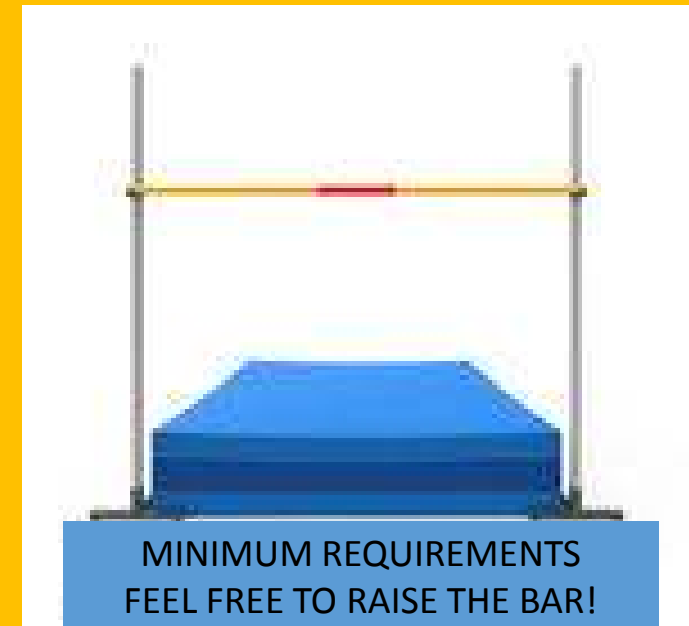
Policy is concerned about granting access to CJI, not about employment.

- ❑ Within 30 days for government employee assignment with DIRECT ACCESS to CJI systems.
 - Own agency or MCA (See 5.1.1.4) with another.
 - Subject to internal agency disciplinary and other policies.
 - Can also control use of information obtained from indirect access.
 - Potentially can be reassigned to job without access to CJI.
- ❑ BEFORE contractor employee is granted ANY ACCESS to unencrypted (plaintext) CJI.
 - Parties are in contractual commitment. (See 5.1.1.5)
 - ❖ Hard to change once work has begun.
 - No other role available for reassignment due to scope of contract.
 - May be out of reach for controlling use or other resolution.

5.12 Policy Area 12: Personnel Security

☐ Finger Print based Record Check

- Finger prints submitted to KBI
 - KBI searches KANSAS records then forwards to FBI
 - FBI searches images associated with III
 - Results will be returned to Agency Primary terminal.
 - QR for any “rap sheet” in III.
 - KFQ for KANSAS CCH.
- QWA Searches all NCIC persons files without limitations.
- Out of State?
 - Run Nlets IQ for state of residency.

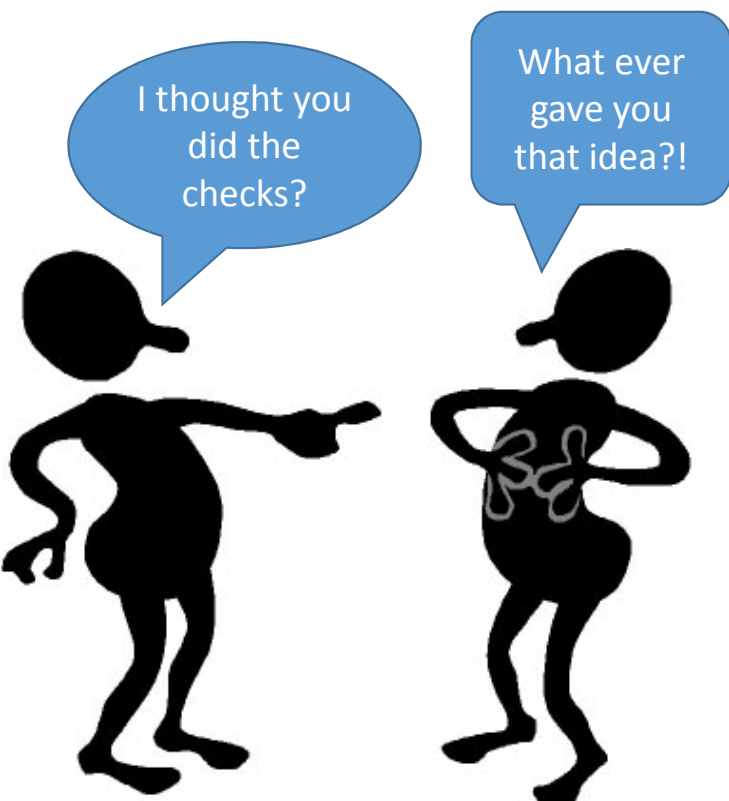


5.12 Policy Area 12: Personnel Security

❑ Name Based Record Check ANNUALLY thereafter
(or when reasonable suspicion that CHRI has changed)

- NCIC Person files (QWA)
- III (QH)
(QWI = QWA + QH)
- Nlets IQ for out of state of residency
- KANSAS wanted
- KANSAS CCH

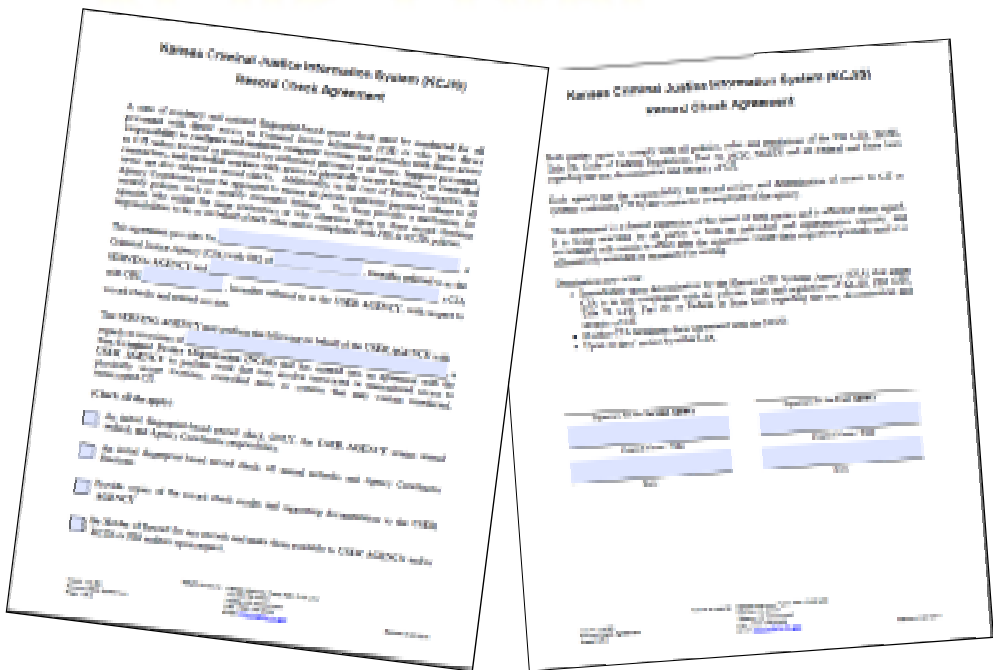


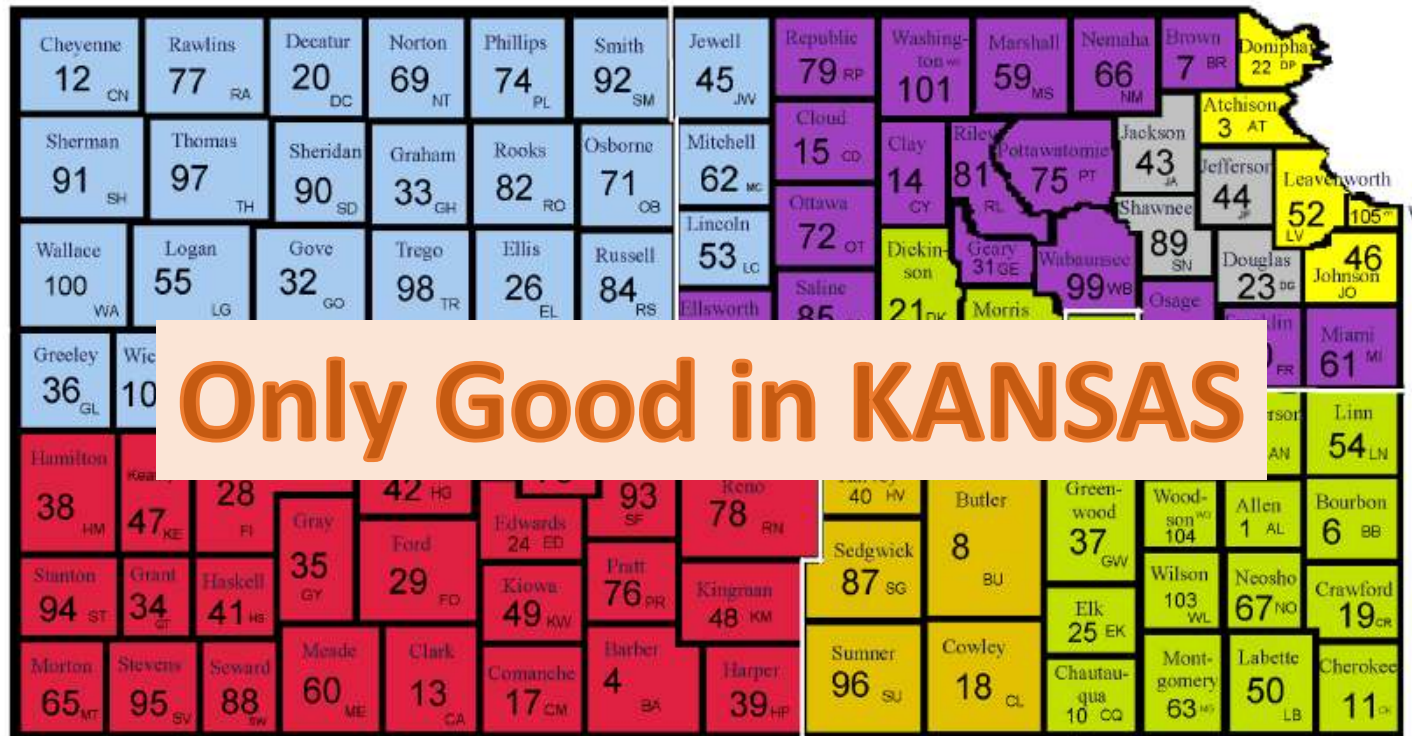


Using same contractors as other CJAs?

KCJIS 114RC

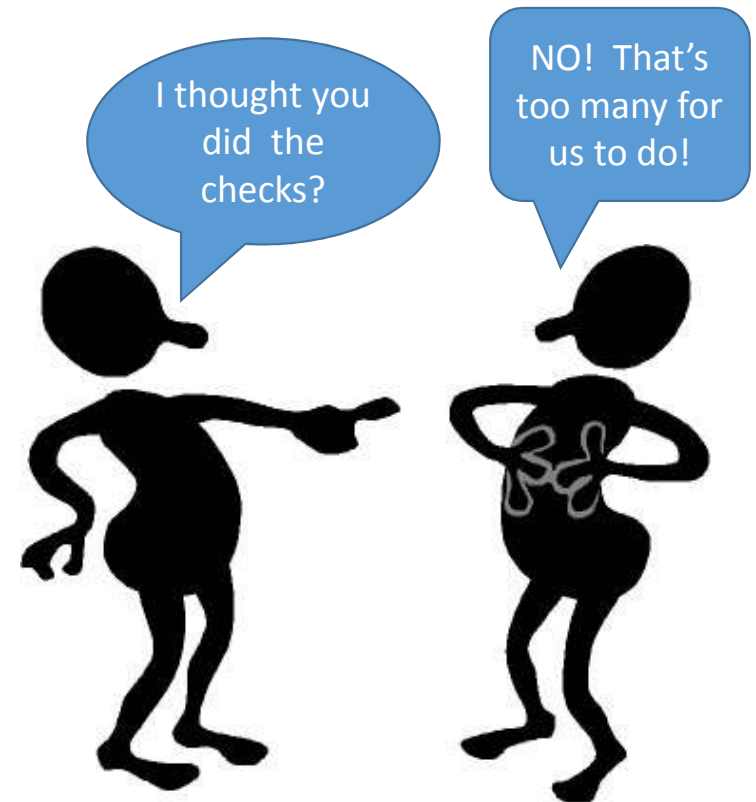
- ✓ Designed specifically so CJAs can share record check results
- ✓ Specifies who does what
- ✓ Creates paper trail for KHP/FBI audits





Using same contractors as lots of other CJAs?

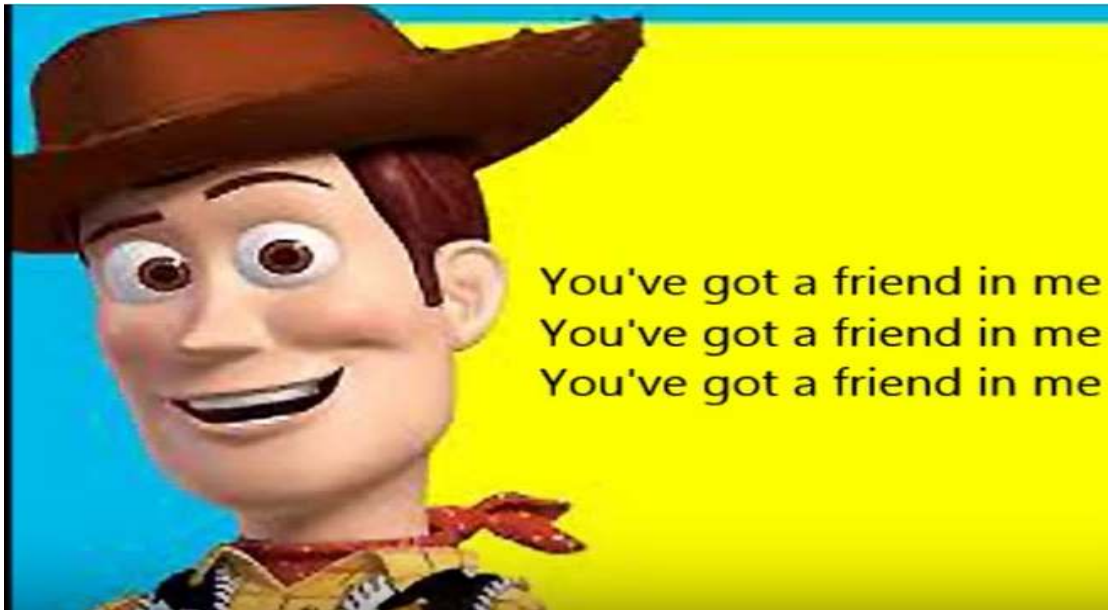
- ☐ Contractor has 3 or more CJA customers.
- ☐ Contractor has 6 or more employees.
- ☐ CJA customers spans jurisdictions.





KANSAS HIGHWAY PATROL

CJIS Unit



Kansas Criminal Justice Information System (KCJIS) Record Check Agreement

A state of residency and national fingerprint-based record check must be conducted for all personnel with direct access to Criminal Justice Information (CJI) or who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI unless escorted or monitored by authorized personnel at all times. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas are also subject to record checks. Additionally, in the case of Private Contractors, an Agency Coordinator must be appointed to ensure all private contractor personnel adhere to all security policies such as security awareness training. This form provides a mechanism for agencies who utilize the same contractors or who otherwise agree to share record checking responsibilities to do so on behalf of each other and in compliance with FBI & KCJIS policies.

This agreement is between the Kansas Highway Patrol (KHP), a Criminal Justice Agency (CJA) with ORI of KSKHPQ000, and _____, a CJA with ORI _____ (henceforth known as the AGENCY).

In regards to associates of _____, a Non-Criminal Justice Organization (NCJO) that has entered into an agreement with the AGENCY to perform work that may involve unescorted or unmonitored access to physically secure locations, controlled areas or systems that may contain unredacted, unencrypted CJI.

On behalf of the AGENCY, the KHP shall perform the following:

- ✓ An initial fingerprint-based record check, all annual rechecks and Agency Coordinator functions.
- ✓ Be Holder of Record for any records and make them available to AGENCY FBI auditors upon request.
- ✓ The KHP shall review all records obtained as part of this process and adjudicate (approve or deny) the subjects access to CJI or systems containing CJI. All adjudications shall be communicated to both the Agency and NCJO through electronic means as marked below.

- ☐ Email
- ☐ CJIS Online
- ☐ Other method _____

PLEASE...
the FD 258 needs to be:

- **LEDGIBLE**
 - Livescan/
machine printed preferred
 - FULL images
- **COMPLETE**
 - LAST, First, Middle
 - Date of Birth
 - Place of birth
 - SOC
 - CURRENT Residence (State)
- **CURRENT**

Image capture date
MUST be within
past 12 months

KHP has cards with our ORI

APPLICANT <small>* See Privacy Act Notice on Back</small> FD-258 (Rev. 9-9-13) 1110-0046 SIGNATURE OF PERSON FINGERPRINTED		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK LAST NAME FIRST NAME MIDDLE NAME KSKHPQ000 HWY PAT STATE HDQTRS TOPEKA, KS				FBI LEAVE BLANK	
RESIDENCE OF PERSON FINGERPRINTED		ALIASES AKA		OR I		DATE OF BIRTH DOB Month Day Year		PLACE OF BIRTH POB	
DATE	SIGNATURE OF OFFICIAL TAKING FINGERPRINTS	CITIZENSHIP CTZ		SEX	RACE	HGT.	WGT.	EYES	HAIR
EMPLOYER AND ADDRESS		YOUR NO. OCA		LEAVE BLANK					
REASON FINGERPRINTED		FBI NO. FBI		CLASS: _____					
		ARMED FORCES NO. MNU		REF: _____					
		SOCIAL SECURITY NO. SOC							
		MISCELLANEOUS NO. MNU							
1. R. THUMB		2. R. INDEX		3. R. MIDDLE		4. R. RING		5. R. LITTLE	
6. L. THUMB		7. L. INDEX		8. L. MIDDLE		9. L. RING		10. L. LITTLE	
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY				L. THUMB		R. THUMB		RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY	

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

6. *Be responsible for securing security awareness training and associated record keeping.*

5.2 Policy Area 2: Security Awareness

- ☐ “roamin’ around” access to areas where CJI is processed or stored.
5.2.1.1 (1-4)
- ☐ ACCESS to plaintext(unencrypted) CJI.
5.2.1.2 (1-6)
- ☐ Physical and logical access to CJI (computer access)
5.2.1.3 (1-17)
- ☐ Unmonitored access to networks used to transmit unencrypted CJI.
5.2.1.4 (1-5)



CUMULATIVE



5.2 Policy Area 2: Security Awareness

- BECAUSE.. People are the weakest link!

- ☐ KHP CJIS Launch Pad

+

- ☐ NexTEST tracks CJIS requirement



Certification Level	Expiration Date
<input checked="" type="checkbox"/> CJIS Security & Awareness	<input type="text"/>
<input type="checkbox"/> Local Agency Security Officer	<input type="text"/>
<input type="checkbox"/> TAC Training	<input type="text"/>

Vendors from out of your area?

Has lots of employees?

Used by several agencies?

- ✓ FREE to local agencies.
- ✓ From the makers of NexTEST.
- ✓ Designed for non-agency personnel.
(No KCJIS user required).

Contact your I.T.S. auditor for details

INTRODUCING!





1. CJIS prescribed levels of awareness

- Vendor maintains CJIS requirements
- “Prefabbed” interactive presentation
- NexTEST style testing.

3. Can register record check date

2. Uses employee’s E-mail as user name

- No wasting of KCJIS GEOCLINT username for outside personnel.
- User sets own password

Add Vendor Employee 1

Company Name:

First Name: *

Middle Name:

Last Name: *

Phone Number:

Level Assignment		
LEVEL NAME	LEVEL DESCRIPTION	ASSIGN
Level 1 CJIS Security Training	All Vendors with Access to CJIS (This level is designed for vendors who do not have physical and logical access to CJIS but may encounter it in their duties.)	<input type="radio"/>
Level 3 CJIS Security Training	Vendors with Information Technology Roles (This level is designed for all vendors with information technology roles including system administration, security administration, network administration, etc.)	<input type="radio"/>

Expiration Notification: ☐

This will allow a vendor employee to manage employees in their company.

Admin Status: ☐

Finger Print Information

Date:

Email address is your user name

Email Address: *

Confirm Email Address: *

Password: *

Confirm Password: *

5.5.4 System Use Notification

At the operating system level, OR....

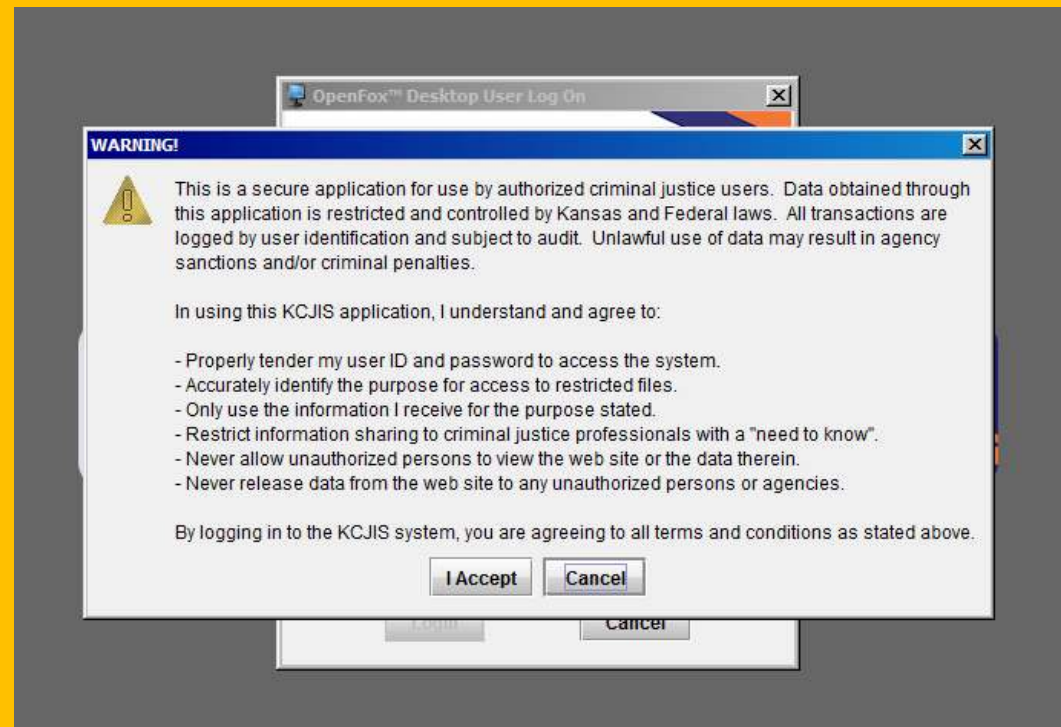
WARNING! – FOR OFFICIAL USE ONLY.

You are accessing a restricted information system.

System usage may be monitored, recorded, and subject to audit.

Unauthorized or inappropriate use of the system is prohibited and may result in discipline up to and including dismissal from employment, civil and/or criminal penalties that may include prosecution.

Use of the system indicates consent to monitoring and recording.



At the application level

5.8 Policy Area 8: Media Protection

5.8.4 Disposal of Physical Media

Authorized User/Personnel — ... who have been appropriately vetted through a national fingerprint-based record check ...

A police department contracts with a document management company to shred their old paper files. The private contractor picks up sheets of plaintext printouts in bins and loads them on a truck to transport to their facility to shred. They return a “certificate of destruction” to the police department.

- ☐ Per 5.12.1.2 - The police department *must record check the truck driver and any other employees or subcontractors of the document company who may have unescorted access* to the plaintext CJI prior to shredding.
- ☐ Those document company employees are *subject to Security Awareness Training* described in 5.2.1.1 & 5.2.1.2

5.8 Policy Area 8: Media Protection

5.8.4 Disposal of Physical Media

Authorized User/Personnel — ... who have been appropriately vetted through a national fingerprint-based record check ...

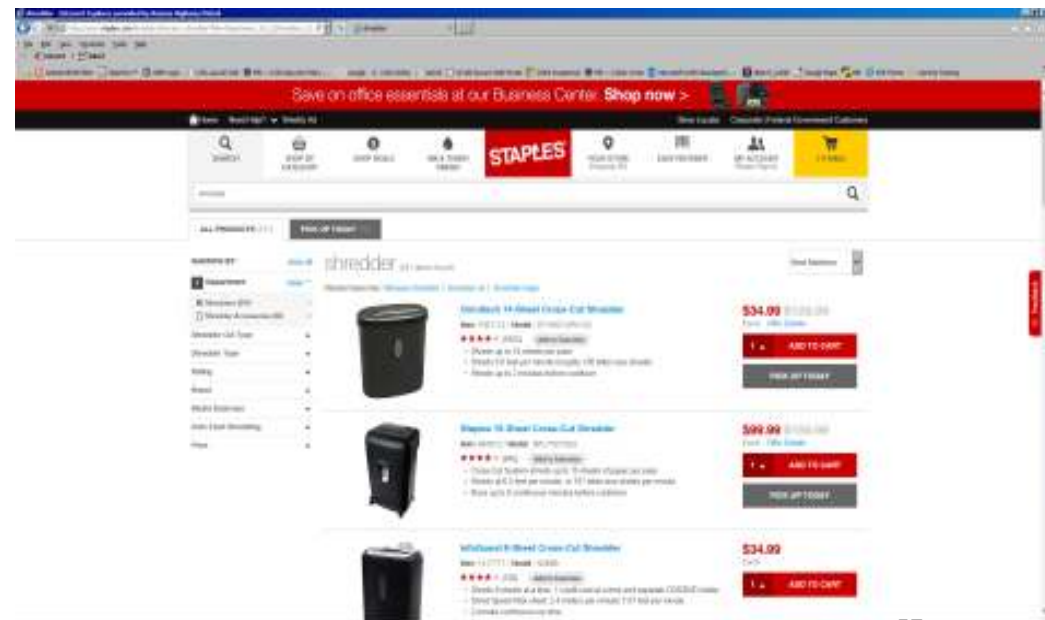
POLICY MITIGATION OPTIONS:

- Change contract for on site shredding where an agency authorized person witnesses the shredding.



Cost too Much?

- Go paperless.
 - Print to PDF
 - Copy + Paste to other application
- Buy a shredder
 - shred your own documents containing CJJ.
 - Destroy A.S.A.P. (see 4.2.4)




5.9 Policy Area 9: Physical Protection

5.9.1 Physically Secure Location



Can both the PHYSICAL and personnel security controls be sufficient to protect CJI?

- ☐ Personnel are record checked and security awareness trained.
- ☐ Can be locked to control physical access
- ☐ Device used to access CJI requires local logon (user id & authentication - i.e. : windows login + password)
- ☐ **NO AA required for local CAD/RMS from these physically secure locations**
- ☐  STILL required to access KCJIS
- ☐ All other policies still apply. (i.e.: encryption)

5.9 Policy Area 9: Physical Protection

5.9.1 Physically Secure Location



Are both the
PHYSICAL and
PERSONNEL SECURITY
controls sufficient to protect
CJI?

No Personnel record checks
+ No Security Awareness training
= NO physically secure location

No Access Controls (locks, etc.)
= NO physically secure location

☐ Device used to access CJI requires
local login (user id & authentication)

☐ **NO AA required for local RMS
(IN-DIRECT access)**

☐ **AA IS REQUIRED for DIRECT access
to CJI (5.6.2.2.1)**

✓ Covered for now ...



5.10 Policy Area 10: System and Communications Protection and Information Integrity

5.10.1.1 Boundary Protection

3. KCJIS policy requires that any **connections to the Internet, other external networks, or non-criminal justice information systems occur through locally managed firewalls**. See Section 5.13.4.4 for guidance on personal firewalls. Also refer to National Institute of Standards and Technology (NIST) Special Publication 800-41 Guidelines on Firewalls and Firewall Policy, available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=901083

(or from the KHP CJIS Launch Pad > CJIS Documents > TECHNICAL SECURITY INFORMATION)

https://cjsiaudit.khp.ks.gov/launchpad/cjisdocs/files/nist_sp800-41_guidelines_on_firewalls_and_firewall_policy.pdf

- ✓ Can be a personal firewall on ALL devices (see 5.13.4.4)
- ✓ NIST SP 800-41 is more current than previous KCJIS information.
- ☐ WIRELESS access is “other external networks”.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

5.10.1.2 Encryption

2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

NOTE in the above “shall” statement - the absence of any reference to ownership or management control.

- b) Encryption shall not be required if ...

Secured CAMPUS

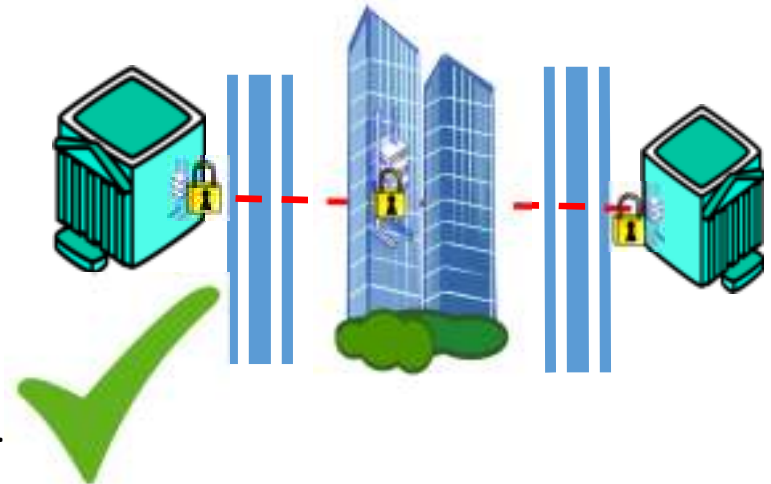
1. Agency controls all areas where cable may be buried.
2. All cables terminate within physically secure locations.
3. All possible paths of buried cable between are in line of sight.
4. **EXEMPT from encryption requirement**

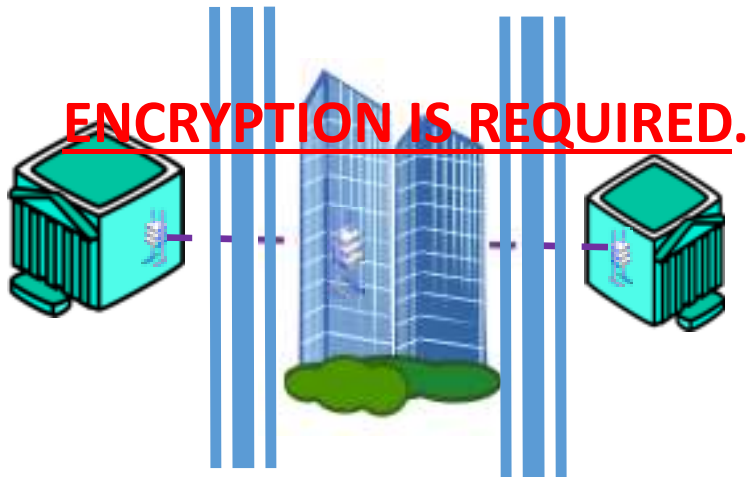


Government Center

Two CJA facilities about 1 block apart. Separated by NCJA (government) building. Government owns and manages fiber.

1. CJA does NOT control all areas where cable may be buried.
2. All paths of cable between are NOT in line of sight.
3. Cables run through concrete and other impenetrable “conduit” into secured facilities (wiring closet or server room) under control of I.T.
4. CJA has MCA with I.T. so all personnel with access are under CJA control.
5. **ENCRYPTION IS NOT REQUIRED.**





Government Center

Two CJA facilities about 1 block apart. Separated by NCJA building. Government owns and manages fiber.

1. CJA does NOT control all areas where cable may be buried.
2. Some cable runs through public access plenum in middle building.
3. Some cables terminate in NCJA areas of middle building.
4. All paths of cable between are NOT in line of sight.
5. There is no controlled campus.

ENCRYPTION IS REQUIRED.



Metropolitan LAN

Two county facilities separated by about 1 mile of uncontrolled city area. County owns fiber.

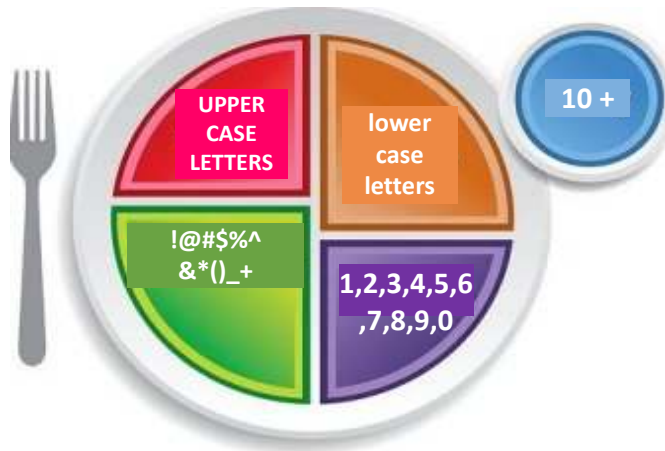
1. Agency does NOT control all areas where cable may be buried.
2. All paths of buried cable between are in line of sight.
3. BUT... Even if there may be line of sight, there is no controlled campus.

ENCRYPTION IS REQUIRED.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

5.10.1.2 Encryption

3. When CJI is at rest outside the boundary of the physically secure location,
- a) ... the **passphrase used** ... shall ...: (be at least 10 characters from all character groups)



(Changed when user no longer needs access)



- b) Multiple files in the same unencrypted folder shall have separate and distinct passphrases.
A single passphrase may be used to encrypt an entire folder or disk containing multiple files.
All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

5.10.1.2 Encryption

4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

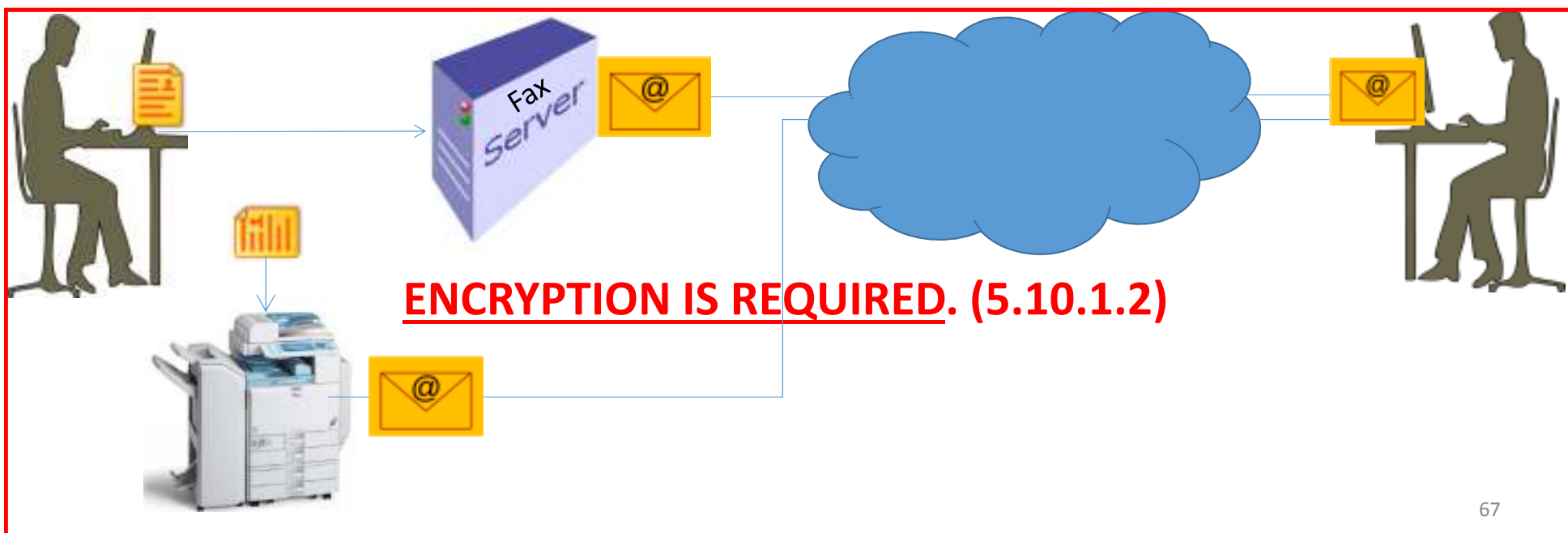
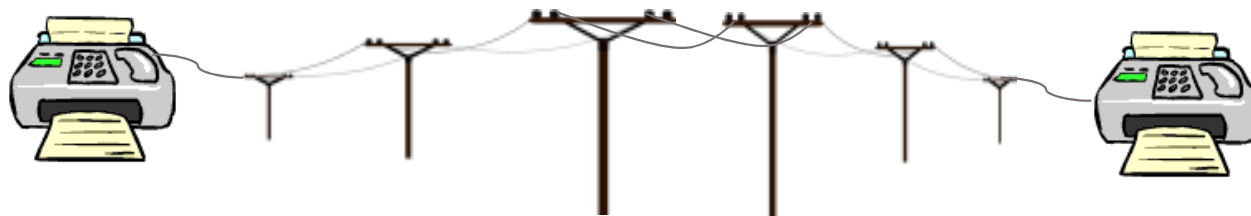
<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm>

EXCEPTION: When encryption is used ***for CJI at rest***, agencies may use encryption methods that are ***FIPS 197 certified, 256 bit*** as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms.

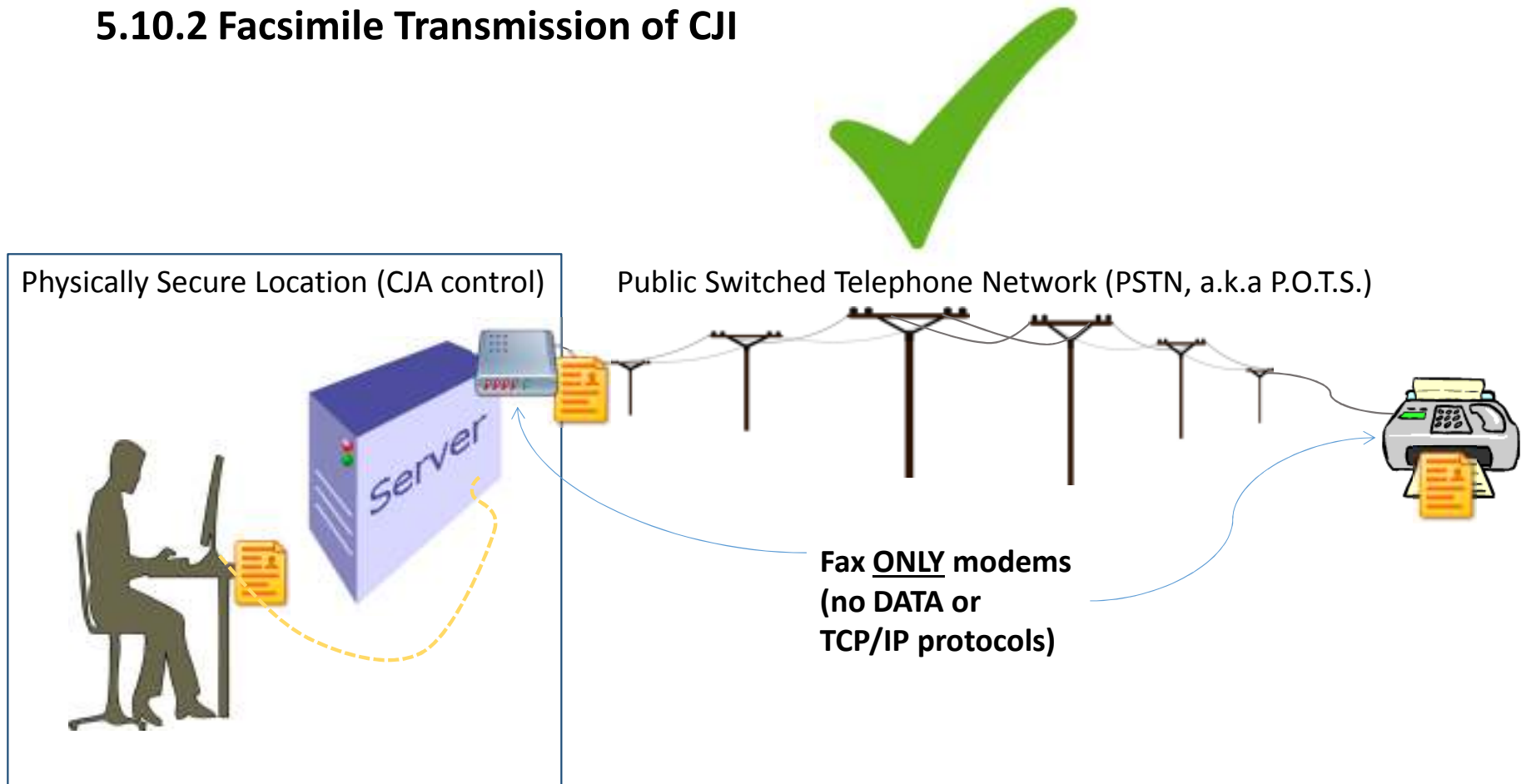
https://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

<http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>

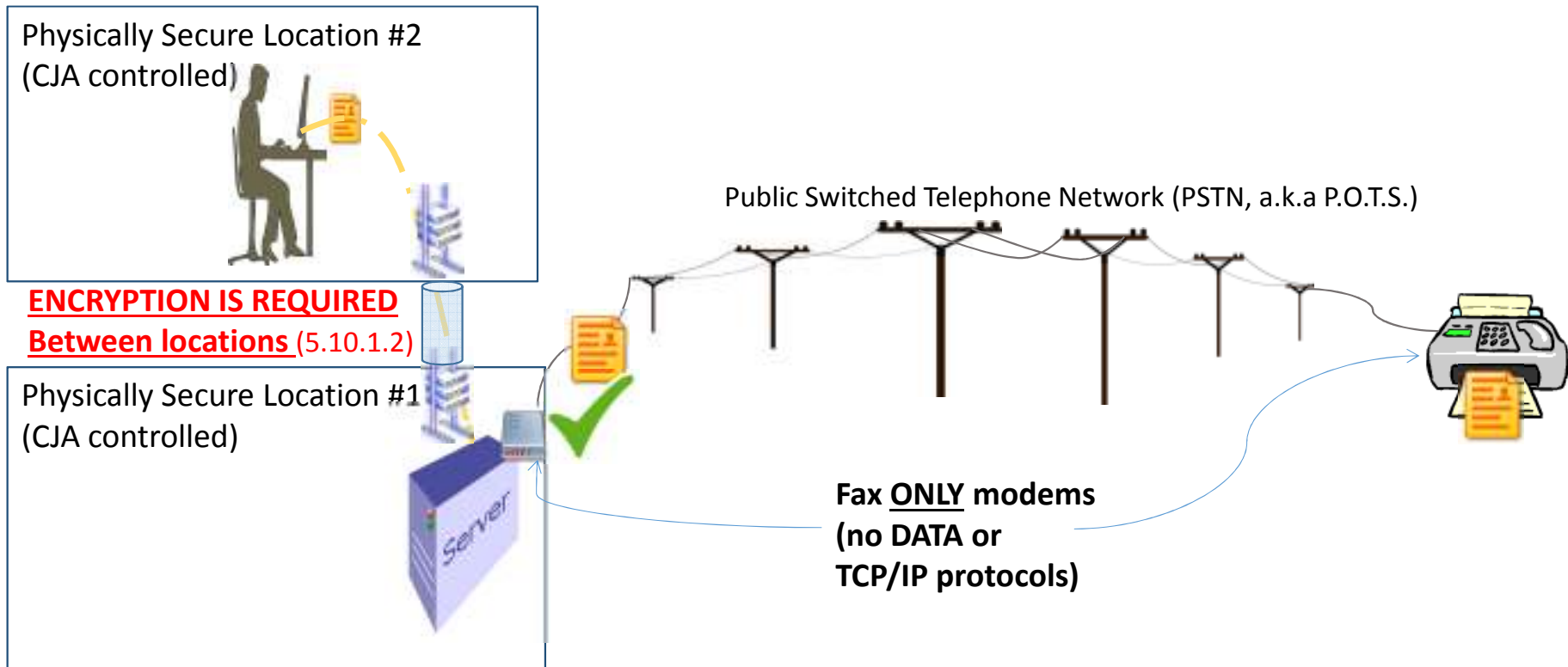
5.10.2 Facsimile Transmission of CJI



5.10.2 Facsimile Transmission of CJI

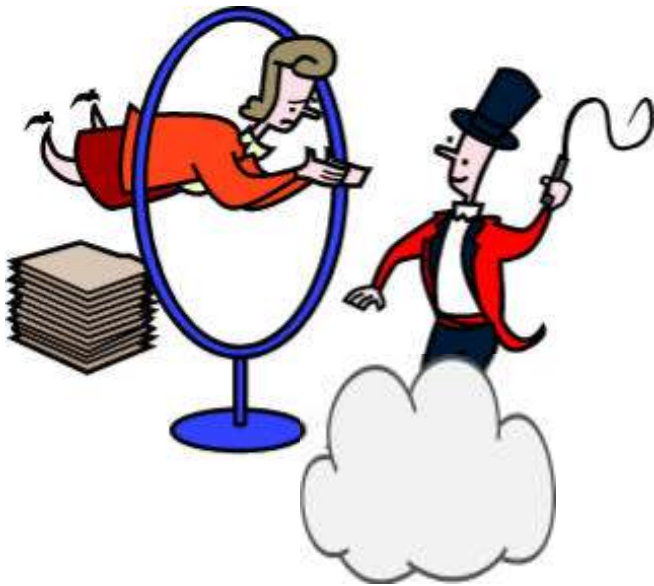


5.10.2 Facsimile Transmission of CJI



5.10.1.5 Cloud Computing

Review the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center <https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view>, NIST Special Publications (800-144, 800-145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.



5.10.4 System and Information Integrity Policy and Procedures

5.10.4.4 Security Alerts and Advisories

<https://www.us-cert.gov/ncas>



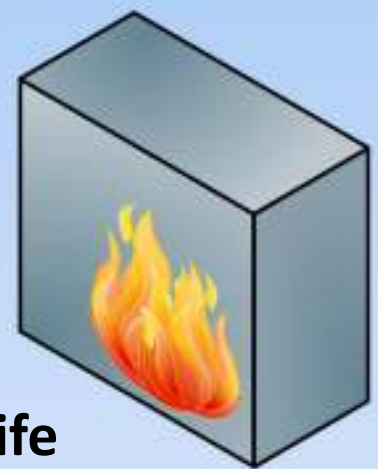
Here's one example/option.

From	Subject	Received
US-CERT	OpenSSL Releases Security Advisory	Tue 3/1/2016 11:06 AM
US-CERT	Apple Releases Security Update for Apple TV	Thu 2/25/2016 6:50 PM
US-CERT	Drupal Releases Security Updates	Wed 2/24/2016 11:36 PM
US-CERT	FTC Shares Security Tips for ASUS Wireless Routers	Tue 2/23/2016 10:12 PM
US-CERT	Microsoft Releases Update for EMET	Tue 2/23/2016 12:13 PM
US-CERT	Google Releases Security Update for Chrome	Thu 2/18/2016 8:25 PM
US-CERT	GNU glibc Vulnerability	Wed 2/17/2016 5:06 PM
US-CERT	Mozilla Releases Security Updates	Fri 2/12/2016 5:15 AM
US-CERT	Cisco Releases Security Update	Thu 2/11/2016 12:09 PM
US-CERT	Microsoft Releases February 2016 Security Bulletin	Tue 2/9/2016 6:21 PM
US-CERT	Google Releases Security Update for Chrome	Tue 2/9/2016 5:56 PM
US-CERT	Adobe Releases Security Updates	Tue 2/9/2016 2:13 PM
US-CERT	Oracle Releases Security Updates for Java	Mon 2/8/2016 5:12 PM
US-CERT	Comodo Chromodo Browsers Vulnerable to Cross-Domain Attacks	Thu 2/4/2016 7:07 PM
US-CERT	SB16-032: Vulnerability Summary for the Week of January 25, 2016	Mon 2/1/2016 10:28 AM
US-CERT	Mozilla Releases Security Updates	Tue 1/26/2016 5:11 PM
US-CERT	IRS Releases Tenth Security Tip	Tue 1/26/2016 12:35 AM
US-CERT	Apple Releases Security Update for tvOS	Tue 1/26/2016 12:10 AM
US-CERT	SB16-025: Vulnerability Summary for the Week of January 18, 2016	Mon 1/25/2016 6:15 AM
US-CERT	Google Releases Security Update for Chrome	Wed 1/20/2016 10:22 PM
US-CERT	Cisco Releases Security Updates	Wed 1/20/2016 5:35 PM
US-CERT	Linux Kernel Vulnerability	Tue 1/19/2016 8:13 PM
US-CERT	ISC Releases Security Updates for BIND	Tue 1/19/2016 8:13 PM
US-CERT	Apple Releases Security Updates for iOS, OS X El Capitan, and Safari	Tue 1/19/2016 8:13 PM
US-CERT	Oracle Releases Security Bulletin	Tue 1/19/2016 5:40 PM
US-CERT	IRS Releases Ninth Security Tip	Tue 1/19/2016 12:10 PM
US-CERT	SB16-018: Vulnerability Summary for the Week of January 11, 2016	Mon 1/18/2016 7:02 AM
US-CERT	OpenSSH Client Vulnerability	Thu 1/14/2016 9:14 PM
US-CERT	Cisco Releases Security Updates	Wed 1/13/2016 8:09 PM

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

Don't forget about the other vulnerable parts of your networks



Vendor announced End of Life

- means no patches available

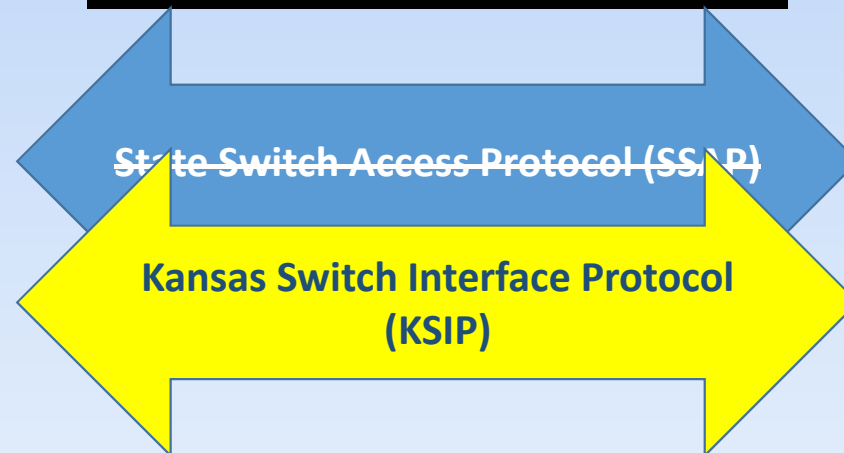
No patches available

- **Means NON COMPLIANT**

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

Speaking of End of Life ... (or if you prefer – “the sunset”)



5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management



Unless you have a



**You Need
A Budget.**

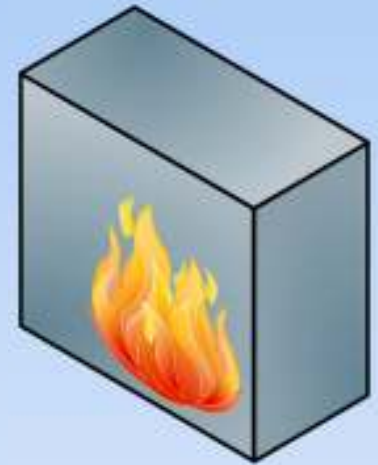


for Equipment and software
upgrades and support *after*
initial funding and contract expires

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.2 Malicious Code Protection

5.10.4.3 Spam and Spyware Protection



at critical points throughout the network and on all workstations, servers and mobile computing devices on the network

5.13 Policy Area 13: Mobile Devices



Accepted FBI CSP as written with one addition to 5.13.1.3 Bluetooth



Bluetooth is not allowed for transfer of CHRI * between computing devices. Bluetooth is allowable for devices such as keyboards, mice, microphones, headsets, etc.



*Refer to definition of CJI in 4.1

- Data entry is NOT CJI (yet)
- Devices that display graphic representation of query result (such as traffic light ) are **OK** 
- E-Ticket printer
 - Subject's name, License #, etc. is same information on hand written ticket.
 - CJIS systems are not usually required to obtain that information.
 - Information on ticket does not reveal additional PII, CHRI, or FBI restricted file information.
 - Printer's format not conducive to additional information like CHRI.



5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

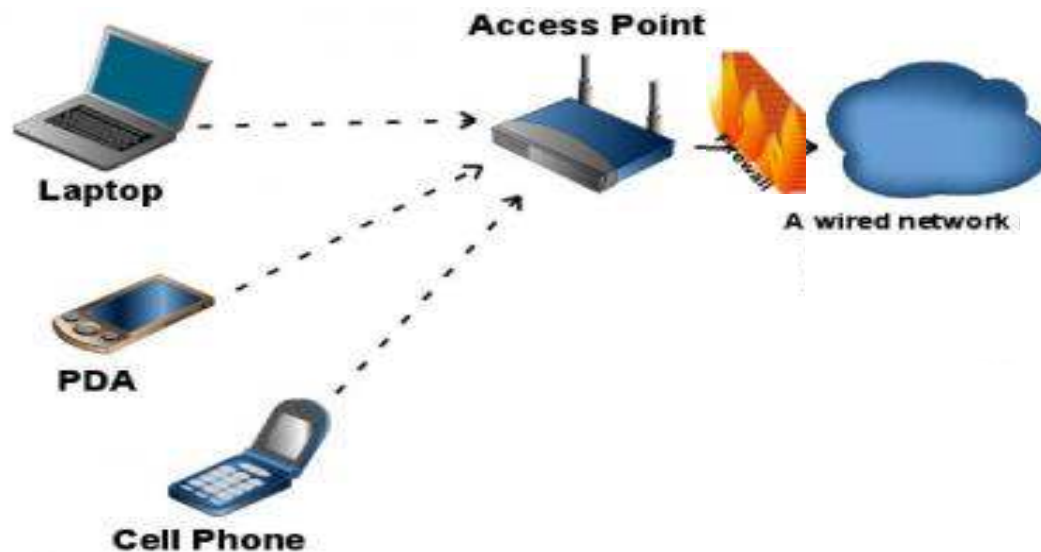
Includes all wireless considerations.

5.13.1.1 All 802.11 Wireless Protocols

5.13.1.2 Cellular

5.13.1.3 Bluetooth

By its nature, wireless communications occur over “external networks” (AIR is *outside* agency control!). See 5.10.1.1 #3 regarding firewalls.



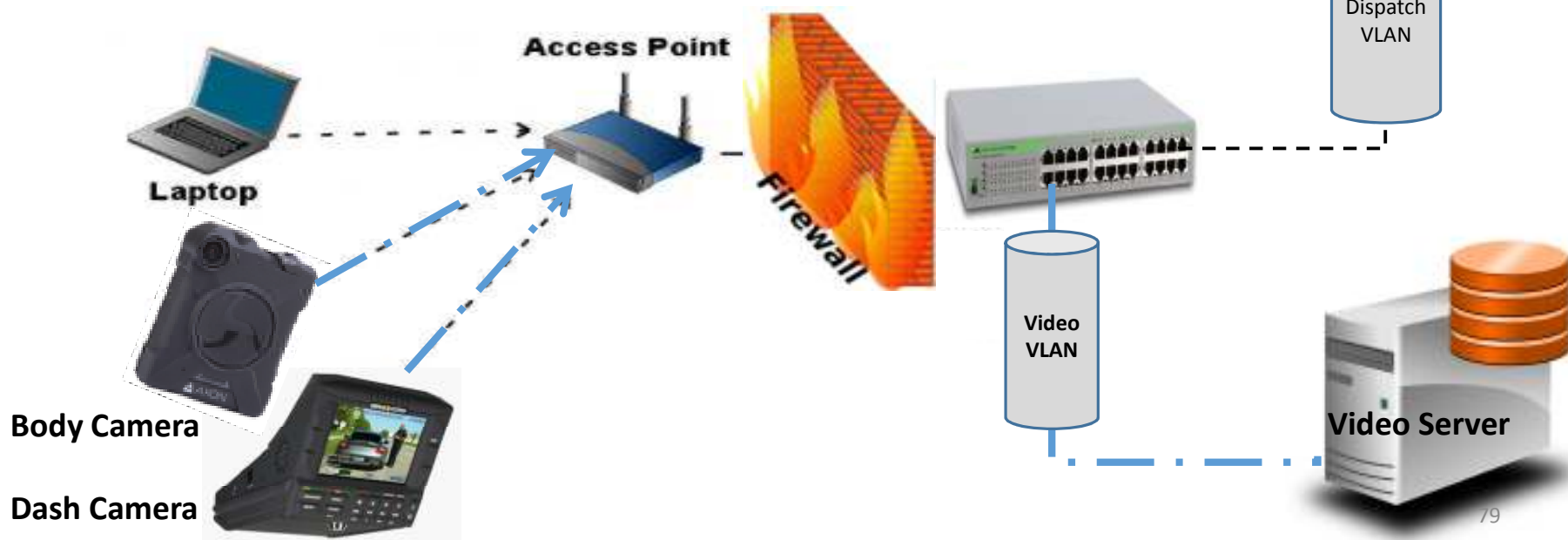
5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

5.13.1.1 802.11 Wireless Protocols

Agencies shall implement the following controls for all agency-managed wireless ***access points with access to an agency's network that processes unencrypted CJI:***

15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure.

Limit access between wireless networks and the wired network to only operational needs.



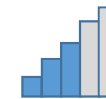
5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

Managing devices accessing your network and CJI

Full Featured vs. Limited Functionality Operating Systems



Connectivity?



Form Factor



5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

Managing devices accessing your network and CJI

5.13.2 Mobile Device Management (MDM)

- ☐ CJI only transferred between authorized applications and storage
- ☐ Centralized administration
 - ☐ Remote Lock
 - ☐ Remote Wipe
 - ☐ Setting and locking device configuration
 - ☐ Detect rooted or jailbroken
 - ☐ Enforce encryption (5.10.1.2)
 - ☐ Apply policies
 - ☐ Detect unauthorized configurations



5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

Managing devices accessing your network and CJI

5.5.6.1 Personally Owned Information Systems

When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.



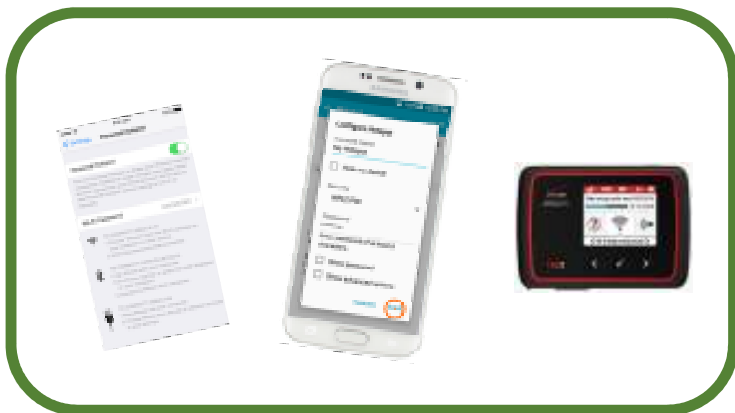
5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

Managing devices accessing your network and CJI

5.13.8 Wireless Hotspot Capability

☐ 5.13.1.1 All 802.11 Wireless Protocols

☐ Only Agency Authorized Devices



=



